AMENDMENTS TO THE CLAIMS

Please amend claims 37, 48, 52-55, 60 and 65 as follows.

Claims 1-36 (Cancelled).

37. (Currently amended) A method comprising:

receiving a first request from a terminal behind a firewall at a secure server outside of the firewall, ~~from a terminal a first request~~ the first request including a composite address, the composite address including an unencrypted address of [[a]] the secure server with an encrypted address of a web page concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal;

transmitting a second request by the secure server to a web site containing the web page, wherein the second request alters or omits an address of the terminal;

retrieving the web page designated in the second request;

modifying an address associated with the retrieved web page by the secure server so that the secure server appears to be the source of the web page and the firewall is unable to determine the address associated with the retrieved web page; and

encrypting the content of the retrieved web page by the secure server and sending the encrypted web page by the secure server, via a secure link, to the terminal, wherein the firewall is unable to decrypt the encrypted content of the retrieved web page.

38. (Previously presented) The method of claim 37 wherein the secure link comprises a secure sockets layer (SSL) link.

39. (Previously presented) The method of claim 37 wherein modifying the address associated with the retrieved web page comprises modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of the web site.

40. (Previously presented) The method of claim 37 wherein modifying the address associated with the retrieved web page comprises modifying an address associated with a hypertext link in the retrieved web page to indicate the address associated with the secure server.

41. (Previously presented) The method of claim 37, further comprising modifying computer code associated with the retrieved web page to cause subsequent requests related to the retrieved web page to be sent by the terminal to the secure server instead of to the web site.

42. (Previously presented) The method of claim 37, further comprising decrypting the encrypted address of the web page.

43. (Previously presented) The method of claim 37, further comprising repeating the retrieving, modifying, encrypting, and sending while the secure link is active.

44. (Previously presented) The method of claim 37, further comprising triggering a deletion of stored electronic files at the terminal related to a communication via the secure link, in response to termination of the communication between the terminal and the secure server.

45. (Previously presented) The method of claim 37, further comprising, at the secure server, controlling transmission of electronic files to the terminal based on preferences received from the terminal.

46. (Previously presented) The method of claim 37, further comprising storing under a pseudonym at a location communicatively coupled to the secure server, electronic files sent with the web page.

47. (Previously presented) The method of claim 37, further comprising:

obtaining information related to a user's communication with the secure server;

providing the obtained information to an entity based on permission of the user and in exchange for providing the secure link; and

providing advertisements from the entity to the user related to the obtained information.

48. (Currently amended) A machine-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to effect the following:

receive a first request from a terminal behind a firewall at a secure server outside of the firewall, ~~from a terminal a first request~~ the first request including a composite address, the composite address including an unencrypted address of [[a]] the secure server with an encrypted address of a web page concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal;

transmit a second request by the secure server to a web site containing the web page, wherein the second request alters or omits an address of the terminal;

retrieve the web page designated in the second request;

modify an address associated with the retrieved web page by the secure server so that it appears that the secure server is the source of the web page and the firewall is unable to determine the address associated with the retrieved web page; and

encrypt the content of the retrieved web page by the secure server and sending the encrypted web page by the secure server, via a secure link, to the terminal, wherein the firewall is unable to decrypt the encrypted content of the retrieved web page.

49. (Previously presented) The machine-readable medium of claim 48 wherein the instructions cause the processor to send the encrypted data via the secure link by sending the encrypted data via a secure dockets layer (SSL) link.

50. (Previously presented) The machine-readable medium of claim 48 wherein the instructions cause the processor to modify the address associated with the retrieved web page by modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of the web site.

51. (Previously presented) The machine-readable medium of claim 48 wherein the instructions cause the processor to:

receive the request from the terminal forwarded from an intermediate unit;

retrieve the web page designated in the request from a source;

modify address information in the retrieved web page to indicate a source address corresponding to an address associated with the intermediate unit rather than to an address associated with the source that provided the web page; and

directly send an encrypted version of the retrieved web page from the secure server to the terminal, via the source link.

52. (Currently amended) ~~An apparatus~~ A secure server, comprising:

a processor coupled to a storage unit, the storage unit being capable of storing a computer program; and

a communication unit to allow the processor to communicate with a terminal behind a firewall, wherein the secure server is outside the firewall, and with a web site outside the firewall, wherein the computer program is capable of directing the processor and the communication unit to:

receive from the terminal a first request including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal:

transmit a second request to the web site, wherein the second request alters or omits an address of the terminal;

retrieve the web page designated in the second request;

modify an address associated with the retrieved web page so that the secure server appears to be the source of the web page and the firewall is unable to determine the address associated with the retrieved web page; and

encrypt the content of the retrieved web page and sending the encrypted web page, via a secure link, to the terminal, wherein the firewall is unable to decrypt the encrypted content of the retrieved web page.

53. (Currently amended) The ~~apparatus~~ secure server of claim 52 wherein the secure link comprises a secure sockets layer (SSL) link.

54. (Currently amended) The ~~apparatus~~ secure server of claim 52, further comprising a database unit communicatively coupled to the processor to store electronic files under a pseudonym, the electronic files corresponding to data sent from the web site along with the retrieved web page.

55. (Currently amended) A method comprising:

receiving from a terminal behind a firewall at an intermediate unit outside of the firewall a first request, ~~at an intermediate unit a first request from a terminal~~ the first request including a composite address, the address including an unencrypted address of a

secure server with an encrypted address of a web page concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal;

forwarding the first request to the secure server;

transmitting a second request by the secure server to a web site containing the web page, wherein the second request includes the web page address and alters or omits an address of the terminal;

retrieving the web page designated in the second request;

modifying an address associated with the retrieved web page by the secure server so that the intermediate unit appears to be the source of the web page and the firewall is unable to determine the address associated with the retrieved web page; and

encrypting the content of the retrieved web page by the secure server and sending the encrypted web page by the secure server, via a secure link, from the secure server to the terminal, wherein the firewall is unable to decrypt the encrypted content of the requested web page.

56. (Previously presented) The method of claim 55, further comprising receiving, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

57. (Previously presented) The method of claim 55 further comprising receiving subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

58. (Previously presented) The method of claim 55, further comprising decrypting the encrypted web page address.

59. (Previously presented) The method of claim 58, further comprising re-encrypting the address associated with the retrieved web page and concatenating the re-encrypted address with the address associated with the intermediate unit.

60. (Currently amended) A machine-readable medium having stored thereon instructions, which when executed by a processor cause the processor to effect the following:

receive from a terminal behind a firewall at an intermediate unit outside of the firewall a first request, ~~at an intermediate unit a first request from a terminal~~ the first request including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal;

forward the first request to the secure server;

transmit a second request by the secure server to a web site containing the web page, wherein the second request includes the web page address and alters or omits an address of the terminal;

retrieve the web page designated in the second request;

modify an address associated with the retrieved web page by the secure server so that it appears that the intermediate unit is the source of the web page and the firewall is unable to determine the address associated with the retrieved web page; and

encrypt the content of the retrieved web page by the secure server and sending the encrypted web page by the secure server, via a secure link, from the secure server to the terminal, wherein the firewall is unable to decrypt the encrypted content of the requested web page.

61. (Previously presented) The machine-readable medium of claim 60, further comprising instructions to receive, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

62. (Previously presented) The machine-readable medium of claim 60, further comprising instructions to receive subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

63. (Previously presented) The machine-readable medium of claim 60, further comprising instructions to decrypt the encrypted web page address.

64. (Previously presented) The machine-readable medium of claim 63, further comprising instructions to re-encrypt the address associated with the retrieved web page and concatenating the re-encrypted address with the address associated with the intermediate unit.

65. (Currently amended) An apparatus comprising:

a first server including a processor coupled to a storage unit, the storage unit being capable of storing a first computer program;

a secure second server including a processor coupled to a storage unit, the storage unit being capable of storing a second computer program;

a first communication unit in the first server, wherein the first communication unit allows the first server to communicate with a terminal behind a firewall, wherein the first server is outside the firewall, and with a web site outside the firewall and with the secure second server outside the firewall, wherein the first computer program is capable of directing the processor and the communication unit to:

receive a first request from the terminal including an address, the address including an unencrypted address of the secure second server with an encrypted web page address concatenated thereto, wherein the terminal encrypted an unencrypted address of the web page provided to the terminal, and

forward the first request to the secure second server; and

retrieve the web page designated in the second request,

modify an address associated with the retrieved web page so that first server appears to be the source of the web page and the firewall is unable to determine the address associated with the retrieved web page, and

encrypt the content of the retrieved web page and send the encrypted web page, via a secure link, from the secure second server to the terminal, wherein the firewall is unable to decrypt the encrypted content of the retrieved web page.

66. (Previously presented) The apparatus of claim 65 wherein the secure second server receives communication protocol information related to a communication between the terminal and the first server, to allow the secure second server to respond to requests sent to the intermediate unit from the terminal.

67. (Previously presented) The apparatus of claim 65 wherein the first server receives subsequent requests from the terminal rather than the secure second server.

68. (Previously presented) The apparatus of claim 65 wherein the secure second server decrypts the encrypted web page address.

69. (Previously presented) The apparatus of claim 68 wherein the secure second server re-encrypts the address associated with the web page and concatenates the re-encrypted address with the address associated with the first server.

70. (Previously presented) A method, comprising:

establishing a secure link between a terminal of a first network and a secure server of a second network, wherein the secure link passes through a firewall of the first network;

receiving at the secure server a request from the terminal for a web page, the request including an encrypted address of the requested web page, wherein the firewall is unable to decrypt the encrypted address;

retrieving the requested web page from a web site containing the requested web page by the secure server, wherein the secure server alters or omits an address of the terminal from communications with the web site;

modifying an address associated with the requested web page so that the address of the requested web page cannot be determined by the firewall; and

encrypting the content of the requested web page and sending the encrypted web page to the terminal via the secure link by the secure server, wherein the firewall is unable to decrypt the encrypted content of the requested web page.

71. (Previously presented) The method of claim 70 wherein modifying an address associated with the requested web page comprises:

modifying the address associated with the requested web page so that the requested web page appears to the firewall to have originated from the secure server instead of the web site.

72. (Previously presented) The method of claim 70, further comprising:

establishing a secure connection between the terminal and a spoofing unit, wherein the secure connection passes through the firewall;

receiving the request at the spoofing unit;

determining the request is destined for the secure server;

forwarding the request from the spoofing unit to the secure server; and

modifying the address associated with the requested web page so that the requested web page appears to the firewall to have originated from the spoofing unit instead of the secure server or the web site.